Controlling the Controller: The Unrelenting Challenge in Digital Shipboard Automation

Mr. Richard A. Holden

This article provides a perspective on shipboard system automation from the aspects of manning, operational use, and acquisition. Automation of naval systems grew from advances in technology made during and just after World War II and has led to profound increases in the operational capability and performance of ships, but it has not notably reduced manning. Shipboard automation is now generally accepted, but the first computer programs used for ship control and weapon control were simply not trusted. Control of the automating element emerged as the central issue when control of machinery was transferred from watchstanders to computers. The issue of dependability created the need for a process to certify shipboard behavior of computers and computer programs. This need to control the automating element led to an institutionalized engineering and acquisition process that was used for decades. Recent reforms in acquisition have eliminated this legacy process and introduced a dependence on commercial hardware and software, again creating the need for a process to certify shipboard behavior of computers and computer programs.

Introduction

This article provides a perspective on the development, evolution, and influence of computer-automated shipboard equipment from the aspects of manning, operational use, and acquisition. Automation of shipboard equipment is one of the principal characteristics of modern warships. Current trends in acquisition associate crew size with total life-cycle cost and insist on greater use of automation to reduce crew size and realize reduced budget goals. A one-to-one correlation of automation and crew size may be an oversimplification since the trade-off between manning and automation is complex. Also, the ownership cost of sophisticated shipboard equipment will influence projected cost savings from smaller crews. Furthermore, automation of safety-critical and mission-critical systems poses a risk to the sailors who use them. The fundamental issue for all automated systems is the possibility of an equipment malfunction caused by an error in the computer program or a failure of hardware. Either cause—error or failure—could lead to hazardous conditions aboard ship, the failure of the ship to carry out its mission, or both. Safety-critical and mission-critical systems must satisfy extraordinary requirements. One example is the automated fire control loop in which equipment controls a system that can take human life; malfunctions cannot be tolerated. Another example is automated propulsion control equipment in which a malfunction could cause loss of mobility and failure to accomplish the mission. Both these examples illustrate the fundamental issue of shipboard automation: quality of the automating element.

IMPACT OF AUTOMATION: MANNING, OPERATION, AND ACQUISITION

Automation of naval systems grew from advances in technology made during and just after World War II. Previously, systems were based on mechanized devices with little internal functionality. Control was provided by manual input, and there was a direct physical linkage between input and output. For mechanized systems, the human operator controlled the system and, thus, provided direct control of the output. The development of computers offered a way for mechanized devices to be self-operating so that direct manual control by a human operator was no longer required. For automated systems, the operator alone does not control the system, but rather the system is controlled by both the operator and the computer. Use of mechanization and automation expands the manual and cognitive capability of sailors, but neither reduces the need for them. Replacing the need for the sailor requires replacing the need for cognitive capability in the first place.

Manning

The number of sailors required to crew ships contributes to the Navy's manpower and, hence, to the total personnel cost. For this reason, the Navy has always tried to limit crew size as a means of limiting total operating costs. Crew size is not arbitrary. A sufficient number of crewmen are needed to effectively operate the ship; that is, to sustain the ship and ensure that its mission can be carried out. Effective operation of the ship will be a function of the manual and cognitive work that the crew collectively performs. Crew training and organization are important factors in determining crew size.[1] However, crew size is limited by the level of technology used and by the mission the ship is expected to perform.

Table 1 gives the crew size for various ships. To compare crew sizes for the ships in this table, a figure of merit is needed. An ideal figure of merit would relate crew size to capability. However, no such figure of merit is available, so a simpler one based on ship displacement per crewman (tons/crewman) will be used. This figure of merit, shown in the last column of Table 1, varies from ship to ship but does not appear to show a large differential

Table 1—Selected Surface Combatants, 1894-1989[2,3,4]

Ship Description	Year Commissioned	Displacement	Crew	Tons/Crewman
Columbia two-masted schooner w/ triple-screw steam	1894	7,375	459	16
Annapolis three-masted barkentine w/ single-screw steam	1897	1,000	135	7.5
Milwaukee Cruiser, Steam Boiler	1906	9,700	664	15
Lexington Cruiser, Steam Boiler	1916	35,000	1,206	29
Fletcher Destroyer, Steam Turbine	1942	2,050	250/300	8/7
Salem Heavy Cruiser, Steam Boiler	1948	17,000	1,200	14
Belknap Guided Missile Frigate, Steam Turbine	1962	6,570	418	16
Spruance Destroyer, Gas Turbine	1975	5,770	319/339	18/17
Oliver Hazard Perry Frigate, Gas Turbine	1977	4,100	206	20
Ticonderoga Cruiser, Gas Turbine	1983	9,466	405	23
Arleigh Burke Destroyer, Gas Turbine	1989	8,300	341	24

with time. Modern ships appear to be only a little more efficient than ships of the past. The technologically advanced ships (the last five in Table 1) average 20.3 tons/crewman compared to the previous ships, which average 13.8 tons/crewman. This apparent reduction in crew size is the combined effect of automation and advanced propulsion technology. Automation and other advances in technology have expanded the manual and cognitive capability of the crew to include more warfighting functions, which have greatly expand the ship's operational sphere. The primary impact of automation does not appear to have been to reduce crew ***size***, but rather to increase crew ***capability***.

The validity of conclusions based on Table 1 will be influenced by sample size. Although only 11 ships are listed, they represent classes of ships, so the sample size is actually larger. Based on the limited analysis presented in Table 1, there appears to have been no major changes in manning levels over the last century, although ships designed in the early 1970s were intended to meet reduced manning requirements. A study of these ships showed that although higher skill levels were required, manning was not reduced to expected levels.[5] This study included six ship classes and reported that actual manning levels were, on average, 18% greater than the final design estimates. Increases from the final design estimates ranged from 4.7% for the DD 993 to 30.5% for the DD 963. This result was disappointing given that, during the 1970s, automation was seen as a means to ultimately realize large reductions in crew size. It was projected[6] that by 1990 advances in technology could reduce essential manning for a destroyer to 62 with partial automation, 42 with extensive automation, and 15 with very extensive automation. Recent papers argue that warship manning requirements can be reduced by the more efficient use of humans and increased use of automation.[7, 8]

Projections of large reductions in manning have not been accurate. One reason is that automation was a necessity of technology advances that created processes which were complex and remote from humans. Technology advances in communications, weapons, and propulsion led to systems that perform processes that cannot be controlled by direct human action; e.g., computations for phased-array radar beam-steering commands. In contrast, cargo handling is a human, hands-on process. Technology advances in weapons and propulsion led to large, complex, computer-controlled systems that could be operated by a few crewmen. Technology advances in other areas have not led to systems that perform sophisticated processes requiring computer control. For example, arming carrier-launched aircraft is a hands-on process performed by sailors on the flight deck. Sustaining the ship at sea remains largely a human, hands-on effort in cargo handling, maintenance and repair, and damage control. Reduced manning will come from developments that lead to a process that requires fewer crewmen to sustain the ship at sea. The computer may be used to automate the new process, but it is the process itself that will reduce manning.

Operation

Automation, as seen from the deckplates, does not involve crew size as much as it involves how people relate to machines. Technology advances not only provided the means for automated mechanization but drove the need for it at the same time. The need for self-operating machines resulted from technology advances made in several different areas, causing increased data volume and reduced response times. Surveillance and communications technology caused an increase in the volume of tactical data available to the sailor, requiring evaluation of large amounts of data that overwhelmed the plot-board-and-grease-pencil approach. Advances in aeronautics led to faster airborne threats with greater ranges of maneuverability and altitude, requiring rapid computation of fire control solutions and quickly slewed gun mounts. The raw cognitive and manual capability of human operators was inadequate and had to be augmented by computers that took over signal processing, weapon servo control, and data management and display.

The development and use of electronic computers overcame human limitations not by replacing them, but by augmenting them by performing humanlike functions. Computers are used to process data and control mechanized equipment in a way that mimics human operators, but much faster, with greater precision, and fewer mistakes. The first digital computers used vacuum tubes and were too large to deploy aboard a ship; therefore, the first automated shipboard systems used analog computers. Development of the solid-state digital computer led to a portable device that was capable enough, yet small enough in size and power consumption to be embedded in systems aboard ships. Digital computers offered advantages over the analog type[9] and were first used for radar signal processors and for tactical data processing tasks that had become difficult or impossible for sailors to do. One of the first automated systems to be deployed was the Naval Tactical Data System, which completed operational testing in April 1962.[10] This system represented the first large-scale change to automation, and the issues that arose in its introduction are fundamental to all computer-controlled shipboard systems. Its introduction was described as an "ultracomplex" change to naval warfare that required special emphasis on overall system control and computer-program error detection and correction.[11]

Following the introduction of the Naval Tactical Data System, shipboard automation was expanded to include digital computer control of machinery. The automated gas turbine was introduced in the 1970s and offered many advantages over the steam plants of the earlier ships—for example, *USS Spruance*, commissioning in 1975, featured automatic starting and central control of the propulsion machinery. Bridge control included main clutch engagement, propeller pitch, and shaft revolutions per minute. In contrast, earlier ships relied on local control of the propulsion machinery, which required watchstanders at various locations to maintain control of pneumatic, hydraulic, and electrical equipment. The digital computer allowed centralized control of the propulsion process, eliminating the need for some watchstanders and, at the same time, ensuring optimum operation of the power plant. Transfer of control of machinery from watchstanders to the computer also raised the issue of reliability. The initial introduction of automated machinery was punctuated with the need for a continuous watchstander and override control[12, 13] to ensure safe operation of the ship.

Shipboard automation is now generally accepted, but the first computer programs used for ship and weapon control were simply not trusted. Targeting and weapon selection were not automatic. Weapons were kept in stand-alone mode, and targets—automatically processed by the Naval Tactical Data System—were manually entered in the weapon system. Therefore, the weapon control process was discontinuous, and as a result, the speed advantage in using the digital computer was lost. The full advantage of the computer was realized when tactical data processing was automatically coupled with the weapon fire control loop. This coupling was accomplished by the Aegis weapon system. First deployed in 1983, the Aegis weapon system relied on the multifunction SPY-1A radar for target detection and fire control. From the first introduction of automatic data processing in 1962, two decades passed before enough confidence could be gained to close the fire control loop with a computer program. And today, with rare exception, shipboard weapons are limited to semiautomatic operation; a final manual action is still required.

The central issue—control of the automating element—drove decisions the Navy made during the 1960s and 1970s.[14, 15] The basic requirement was to guarantee that the automating element did what it was supposed to do and ***only*** what it was supposed to do. Afloat commanders needed assurance that the correct computer inputs would always be given, and that the computer would always provide the correct outputs. To the afloat commander, the computer and its program was a box that converted input to output. The box could not be trained, as was the watchstander it augmented or replaced, and it was impossible to *see* inside the box. A way to determine if the box would function as expected was beyond the afloat commander's reach. Hence, the automating element was perceived as a ***black box*** that had to be depended on to work correctly if its assigned mission was to be safely completed. Therefore, naval officers insisted that computer program maintenance be collocated with training—at Dam Neck and San Diego—and controlled by the fleet. In these early days of automation, the computer and its program were akin to a human crew member, since it performed duties a watchstander would otherwise have had to do.

Eventually the task of computer program maintenance was transferred from fleet training to the systems commands. Thus for the first time, engineers ashore were responsible for the real-time behavior of deployed systems. The deployed commander controlled the human elements of his crew but not the computer programs that he had to depend on to operate certain equipment. A shore-based administrative and engineering procedure was established to guarantee that deployed computers, like deployed sailors, would perform their work as expected. The administrative procedure testified that the engineering procedure had established the exact state, or behavior, of the computer programs before they were installed in deployed systems. The process of certifying computers and computer programs was born as a necessity of automated weapons. Today, this task is critical for in-service ships. Each of the *Ticonderoga* and *Arleigh Burke* class Aegis ships have more than 400 different computer program media aboard. In the combat system alone, not counting firmware, there are at least 45 different computer programs that execute in real time. Support for these programs is the current responsibility of several Navy groups, assisted by contractors. Many of the computer program media and over half of the real-time executable programs are the responsibility of the Naval Surface Warfare Center, Dahlgren Division (NSWCDD) and the Naval Sea Systems Command.

Acquisition

The first applications of computer automation were for dynamic, real-time control of weapon directors and for tactical data processing for threat assessment and weapon selection. Both these applications demanded a high degree of confidence derived from knowledge of the computer and computer program. Deployed commanders could be held accountable for personnel and equipment under their command, but they could not be held accountable for the interworkings of black boxes that controlled their weapons; therefore, the shore establishment was forced to accept responsibility for computer programs installed aboard ships. Safe completion of the assigned mission was no longer the sole responsibility of the afloat commander. The acquisition agent who delivered equipment to the ship would be required to testify that the deployed equipment would work as expected—and be accountable if it did not. If the potential risk to the ship and crew was to be qualified, the automating element could not be a black box. Its internal workings had to be clearly understood and carefully controlled; knowledge of the internal design of the automating element was required, and quality had to be certified.

Certification drove the engineering process and established an acquisition approach for automated tactical systems. The decades following World War II institutionalized this approach to the extent that procedures were followed without a clear connection to the underlying purpose. Engineering automated military systems became a slow, expensive, and cumbersome process. The central issue of the engineering-dominated process—control of the automating element—became hidden and unclear to both practitioners and critics. However, continuation of the Cold War supported continuation of the process as a reliable means to meet justified military needs. Eventually, the approach took on the appearance of a traditional process that required direct military expenditures with little economic advantage to the nonmilitary sector. The end of the Cold War offered an opportunity to remedy what were perceived as costly and unnecessary steps in defense acquisition.

The engineering and acquisition process that evolved from the 1950s had institutionalized processes that ensured systems were certified. These processes were dismantled by acquisition reform[16] in the early 1990s. Under acquisition reform policy, the original requirements used to ensure quality—technical data rights, security, specifications, and standards—are viewed as inhibitors to acquiring the most cost-effective and capable military systems. The desire to improve military procurement was, in the case of automated systems, coupled to the availability of commercial computer hardware and software. In the 1960s, the Navy had to develop its own computer technology, but by the mid-1980s there was general use of computers in the commercial and private sector for office and business automation. The availability of low-cost, commercial computer hardware and software was perceived by the proponents of acquisition reform to have overcome the need for unique military computer equipment. Reduced military budgets could be achieved by streamlining the research, development, and testing process and by using commercial computer products in shipboard systems. The central issue—control of the automating element—was eclipsed by the desire to reduce cost.

The past, or legacy, approach has been replaced by the reengineered acquisition process that is based on use of commercial products to the greatest extent possible. There are numerous technological and financial advantages of using commercial-off-the-shelf products for the automating elements of tactical systems. However, from a systems engineering standpoint, there are difficulties in integrating commercial products into systems. For typical commercial products bought off the shelf, the detailed design is not disclosed to the buyer. Also, design specifications and design changes are under the control of the vendor. For these reasons, only the exterior of commercial-off-the-shelf products is *seen* by the buyer. Unless the vendor discloses the internal design, the buyer purchases a black box.

Much of the financial advantage of using commercial products is gained when they are purchased and used as black boxes to the maximum extent. However, use of commercial products does not remove the need to certify tactical systems to the afloat commander. The issue is: What is the maximum extent that commercial products can be used as black boxes in certifiable systems? The unconstrained legacy approach that simply eliminated all black boxes is not affordable. Thus, a new approach is needed that can be applied to current and future systems. Acquisition reform and affordability requires the central issue—control of the automating element—to again be the basis of a new administrative and engineering process in order to ensure the safety and performance of mission critical systems.

CONTROLLING THE CONTROLLER

Shipboard systems are under the control of watchstanders, who are expected to follow prescribed procedures, are supervised, and are held accountable. Watchstanders are under the direct control of their shipboard superiors who gain confidence in their reliability and performance by training and evaluation. For a computer-automated system, there is an additional layer of control between the watchstander and the system as shown in Figure 1. The operation of this inanimate controller is determined by the real-time behavior of a computer and its program. Characteristics of this controller—the computer and its program—are determined during design, development, and production. Thus, the controller is controlled by the process used to design, develop, produce, and support it. The watchstander must accept the controller's real-time behavior and trust it to be available, reliable, and repeatable. To ensure this trust, the computer and its program should be subjected to a quality-assurance process. Controlling the controller requires engineering to certify that it meets requirements and that the level of risk in using it aboard a ship can be tolerated.

Certifying behavior of an automated system means that the risk in using it has been qualified. To qualify risk, three things must be done:

- Define the system's risk criteria
- Verify the system meets the definition
- Testify to the fidelity of the verification

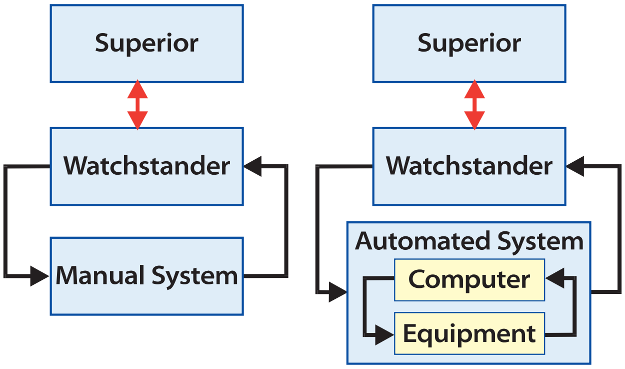

Figure 1—Manual and Automated System Control

The first, defining risk criteria, means specifying an acceptable requirement or standard that can be measured. The second, verification, means determining that design data and test data are accurate and consistent with the documented standard. The third, testifying, means the human act of attesting by report, letter, or other means that the system has met the standard within specified limits. The act of certifying includes the acceptance of accountability and liability for the deployed system, and responsibility for the certification process, including the standard criteria used.[17]

Certification requires that, from the very start of automated system development, attention be given to those malfunctions that can cause safety hazards or mission negation. The severity of safety hazards are easily defined as damage or destruction of the system, injury to people, or loss of life. Mission negation means that (1) the system was necessary to accomplish a specific military mission, and (2) a malfunction could render the system unusable, preventing successful completion of the mission. Careful attention should be given to critical components whose malfunction can cause safety hazards or mission negation. If the system can be redesigned to eliminate all critical components, then all is well. If critical components cannot be eliminated, then the risk of a safety hazard or mission negation can be qualified in terms of eliminating, predicting, and controlling malfunctions. There are well-known engineering methods for risk assessment and management that can be applied throughout the system life cycle to certify that system quality assurance has been met.[18]

Certification does not mean that the automating components of the system are free of all imperfections and will work perfectly. In reality, all systems can and will suffer from components that malfunction due to wear, design defects, and incorrect operating conditions. The malfunction of different system components may lead to different failure mechanisms of the system. One component malfunction may have minimal effect, causing only slight system performance degradation, whereas a different component malfunction may be catastrophic and result in destruction of the system and loss of life. Thus, a given system design can be evaluated to determine the impact of a malfunction of any of its components. System acquisition must deal with a fact of life—the inevitability of malfunctions.

Consider a single component in a multicomponent system. The component is a box that has input and output, performs some function, and is connected to other boxes. Internally, the box may contain a single element or many interconnected elements. There are two types of malfunctions that could occur: hardware or software.

Hardware—The box contains only mechanical or electrical elements; that is, there is no computer program. Used over and over, some element in the box will finally wear out, and the box will malfunction and cause the output to be incorrect. The failure mechanism—wear-out—is stochastic, and repeated testing with copies of the box will establish a rate of failure. Statistical accuracy requires all copies of the box—those tested and those used in the deployed system—to be built to the same design and tolerance. Confidence in predicting failure rate will be based on the quality assurance process used to ensure that all copies of the box are the same.

Software—The box is a computer executing complex software instructions. If the box is used over and over, the software instructions will be executed over and over and in different combinations. Unlike hardware, the instructions cannot wear out, so if there are no errors, the box will operate forever without malfunctioning. If there are errors, then a malfunction can occur. There are generally two types of errors: (1) programming mistakes and (2) inadequate programming. The latter occur in complex programs because of the large number of possible logic paths through the program, which makes it very difficult to consider all possible combinations that can occur when the program is used. For large, complex programs, the programming logic can be expected to fail for some operating conditions that correspond to unique instruction combinations. Computer program failures do not occur at random. The failure mechanism is not stochastic. The cause of the failure is an event-driven condition, which means that malfunctions cannot be predicted statistically from test data. Defects that cause failures are latent defects; they remain hidden until certain operational conditions occur.

These examples illustrate the basic difference in quality control of system hardware and software. Certification of hardware components of automated systems can be accomplished by traditional quality assurance methods used to predict failure rates. Ensuring availability and reliability of hardware used in automated systems is basically the same as for manual systems. Automation has not introduced any fundamentally new or different requirements for quality assurance of deployed hardware. In contrast, the introduction of computer programs in deployed systems requires a new and different approach to quality assurance. Availability, reliability, and repeatability of the computer program are fundamental requirements for automated systems. And the requirement of the quality assurance process is to deal, not with a product that wears out, but with a product that contains latent defects.

Defects in computer programs cannot be entirely prevented so the engineering process will have to be one that can detect, eliminate, and manage latent defects. Software assurance is critical to automation and must be rigorously applied throughout the development and maintenance process.[19] The number of latent defects will invariably grow with the size and complexity of computer programs needed to automate shipboard systems. The expanded use of shipboard automation, particularly as a means of reducing shipboard manning, will lead to the need for greater amounts of software. The challenge is to control computer program quality by continuing to sustain a carefully controlled process for their design, development, production, and maintenance.

A new approach to acquiring and supporting mission-critical systems must be derived from melding together the basis of the legacy approach with the reality of acquisition reform. The legacy approach was based on the conviction that risk must be known, understood, and acceptable. Furthermore, the legacy approach recognized that responsibility and government are inseparable. Today, acquisition reform recognizes that military systems can be made affordable by the use of commercial products. A new engineering and acquisition approach is needed that can deliver affordable and usable commercial-based systems. Affordability depends on the availability of low-cost, high-performance computer hardware and software that can be readily adapted to the warship environment. Usability of commercial-based systems depends on accommodating unique requirements that include supportability and reliability in the warship environment. The need for quality assurance of the computer program has been discussed at length, but other warship environmental factors are equally important. These factors include the effects of shipboard electrical power, electromagnetic interference, and mechanical shock—all of which differ from that experienced in the commercial world. Also, there is no commercial equivalent to battle-short; i.e., in a combat emergency, some systems are required to be operated beyond their normal combat performance limits. Developing commercial-based systems will depend on carefully planned engineering and acquisition that takes full advantage of commercial products while accommodating the warship environment.

CONCLUSION

Automation has greatly increased performance and capability, but it has not yet markedly reduced shipboard manning. The use of automated weapons has impacted the engineering and acquisition process forever by requiring a highly disciplined, shore-based infrastructure to be responsible for the performance of deployed systems. The current issue of affordability underscores the need for the shore-based infrastructure to institutionalize an effective process to certify the performance and safety of deployed systems. The use of computers in critical shipboard systems requires standards, design data, test data, and analysis sufficient to verify performance and to qualify the potential risk to the sailors who use them.

The single most critical requirement for computer-controlled shipboard systems is that the delivery agent is accountable for operational performance and, as a consequence, accepts certification responsibility. The potential danger in not certifying was clearly stated more than 30 years ago: *"The compulsory feature of this situation is that the commander must constantly and carefully monitor the planned programs inserted into this equipment. Unless this is done, incorrect solutions will result, thereby leading to an erroneous decision."*[14] This statement is still valid today—no technology or process has been devised that can repeal it. Certification of systems used aboard warships is still a fundamental requirement of the engineering process, regardless of the acquisition approach taken. The central issue—control of the automating element—is invariant.

ACKNOWLEDGMENTS

Invaluable review comments were received from Neal Cain of NSWCDD. The author is also indebted to all those who participated in the NDI/COTS Workshop conducted at NSWCDD in October 1996[20, 21] and the Workshop Next Step Team: John Allender, James Blackwelder, Neal Cain, Meade Corder, Karole Davidson, Joel Fries, Mike Gallier, J.B. Gessler, Jose Gonzalez, Larry Graeber, Jeff McConnell, Kenneth Powell, and Heath Taylor.

REFERENCES

1. Militello, Laura G. et al., "Optimized Manning Case Studies," Contract N61339-97-C-0066, Subcontract No. 0003, Klein Associates Inc., Fairborn, OH, 6 Oct 1998.
2. Alden, John D., *The American Steel Navy*, Naval Institute Press, Annapolis, MD, 1972.
3. Friedman, Norman, *U.S. Cruisers*, Naval Institute Press, Annapolis, MD, 1984.
4. *Jane's Fighting Ships*, Jane's Information Group, Alexandria, VA.
5. Mellis, James G. et al., "Is Automation the Magic Potion for Manning Problems?," *Naval Engineers Journal*, p. 127, Apr 1982.
6. Fulton, LCDR W. Lawrence, II, USN, "Essential Manning—Its Impact on Destroyer Design, Operation and Maintenance," *Naval Engineers Journal*, p. 79, Jun 1974.
7. Baumann, G. et al., An Arsenal Ship Design, *Naval Engineers Journal*, p. 85, Nov 1997.
8. Anderson, D.E. et. al., "Recapitalizing the Navy Through Optimized Manning and Improved Reliability," *Naval Engineers Journal*, p. 61, Nov 1998.
9. May, CDR Robert E., USN, "Digital Computers in Weapon Control," *U.S. Naval Institute Proceedings*, p. 126, Jan 1964.
10. Swenson, CAPT Eric, USNR (ret.) et al., "NTDS —A Page in Naval History," *Naval Engineers Journal*, p. 53, May 1988.
11. Chapin, G.G., *Sperry Engineering Review*, Summer 1963 issue, Reprinted in *Naval Engineers Journal*, p. 231, Apr 1964.
12. Clayton, Curtis T., "A Practical Approach to Ship Automation," *Naval Engineers Journal*, p. 109, Feb 1964.
13. Mericas, E.C., Commander, USNR, "A Retrospect on Automation in Marine Engineering," *Naval Engineers Journal*, p. 759, Oct 1967.
14. Hayward, VADM John T., USN and Keaney, LTJG Paul J., USNR, "Command and Control in the Nuclear Age," *U.S. Naval Institute Proceedings*, p. 38, Nov 1963.
15. Eckhart, CDR M., Jr., USN, "The Wit to See," *U.S. Naval Institute Proceedings*, p. 34, Aug 1964.
16. Perry, William, The Secretary of Defense Acquisition Reform Memorandum, 15 Mar 1994.
17. Arnston, S., et al., "Arsenal Ship Program Certification Plan," *Naval Engineers Journal*, p. 249, Jan 1998.
18. Roland, Harold E. and Moriarty, Brian, *System Safety Engineering and Management*, John Wiley & Sons, Inc., New York, 1990.
19. *Naval Surface Warfare Center Dahlgren Laboratory Software Process Improvement Tactical Plan*, NSWCDD/MP-97/209, Dec 1997.
20. Summary Report of the NSWCDD Technical Workshop "Re-engineering Weapon Systems— The NDI/COTS Computing Challenge," Dahlgren, VA, 24-25 Oct 1996.
21. Recommendations of the NSWCDD Technical Workshop "Re-engineering Weapon Systems— The NDI/COTS Computing Challenge," Dahlgren, VA, 24-25 Oct 1996.

THE AUTHOR

MR. RICHARD A. HOLDEN

Mr. Richard A. Holden is a system engineer in the Surface Ship and System Engineering Division of the Combat Systems Department. He earned a B.S. degree in physics and mathematics from Arkansas Polytechnic College, an M.S. degree in physics from Southern Illinois University, and completed additional graduate work in physics at the University of Illinois. He worked for Delco Electronics before joining NSWCDD. He has participated in numerous projects ranging from laser technology to upgrade of the Aegis combat system and is currently involved in special system engineering projects and initiatives.